Robin L. Cohen (rcohen@kasowitz.com)
Adam S. Ziffer (aziffer@kasowitz.com)
Alexander M. Sugzda (asugzda@kasowitz.com)
KASOWITZ, BENSON, TORRES &
FRIEDMAN LLP
1633 Broadway
New York, New York 10019
Tel: (212) 506-1700
Fax: (212) 506-1800
Attorneys for Plaintiff Medidata Solutions, Inc.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MEDIDATA SOLUTIONS, INC. Plaintiff, v. FEDERAL INSURANCE COMPANY, Defendant.	Civil Action No.: 1:15-cv-00907-ALC

PLAINTIFF MEDIDATA SOLUTIONS, INC.'S STATEMENT OF UNDISPUTED FACTS PURSUANT TO LOCAL CIVIL RULE 56.1 IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT AGAINST DEFENDANT FEDERAL INSURANCE COMPANY

Pursuant to Local Rule 56.1, Plaintiff Medidata Solutions, Inc. ("Medidata"), respectfully submits this Statement of Undisputed Facts in support of its motion pursuant to Federal Rule of Civil Procedure 56 for summary judgment that Defendant Federal Insurance Company ("Federal") breached its insurance policy obligation to pay up to $5 million for the loss Medidata sustained as a result of a fraudulent wire transfer on September 16, 2014.

I. The Federal Insurance Policy

1. In exchange for a $31,400 premium, Medidata purchased Federal Executive Protection Portfolio Policy No. 8212-1392 for the policy period June 25, 2014 to June 25, 2015 (the "Policy"). (Joint Exhibit Stipulation ("Ex. Stip.") Ex. 1, at FIC001322, 1327.)

2. The Policy contains a Crime Coverage Section that contains ten Insuring Clauses that provide coverage for loss caused by various criminal acts, including Forgery Coverage Insuring Clause 4, Computer Fraud Coverage Insuring Clause 5, and Funds Transfer Fraud Coverage Insuring Clause 6. (*Id.* at FIC001340.)

3. The Policy provides one "Limit of Liability" applicable to its Forgery Coverage, Computer Fraud Coverage, and Funds Transfer Fraud Coverage of $5,000,000, subject to a $50,000 retention. (*Id.*)

4. The Policy defines "**Money**" as "currency [or] bank notes."[1] (*Id.* at FIC001346.)

5. The Policy defines "**Organization**" as "any organization designated in Item 4 of the Declarations for this coverage section." (*Id.*)

6. Item 4 of the Declarations for the Crime Coverage Section lists "Medidate [sic] Solutions, Inc., and its subsidiaries." (*Id.* at FIC001340.)

7. The Policy defines "**Third Party**" as "a natural person other than: (a) an **Employee**; or (b) a natural person acting in collusion with an **Employee**." (*Id.* at FIC001347.)

8. The definition of "**Computer System**" includes "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned and

[1] All emphasized terms appear in boldface in the Policy.

operated by an **Organization**; (b) leased and operated by an **Organization**; or (c) utilized by an **Organization**." (*Id.* at FIC001374.)

9. The Policy's Computer Fraud Coverage Insuring Clause 5 covers "direct loss of **Money**, **Securities** or **Property** sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**." (*Id.* at FIC001342.)

10. The Policy defines "**Computer Fraud**" as: "[T]he unlawful taking or the fraudulently induced transfer of **Money**, **Securities** or **Property** resulting from a **Computer Violation**." (*Id.* at FIC001343.)

11. A "**Computer Violation**" includes both "the fraudulent: (a) entry of **Data** into . . . a **Computer System**; [and] (b) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format . . . directed against an **Organization**." (*Id.* at FIC001343-44.)

12. "**Data**" is defined under the Policy to include any "representation of information." (*Id.* at FIC001344.)

13. The Policy's Funds Transfer Fraud Coverage Insuring Clause 6 provides coverage for "direct loss of **Money** or **Securities** sustained by an **Organization** resulting from **Funds Transfer Fraud** committed by a **Third Party**." (*Id.* at FIC001342.)

14. The Policy defines "**Funds Transfer Fraud**" as: "[F]raudulent electronic . . . instructions . . . purportedly issued by an **Organization**, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Organization** at such institution, without such **Organization's** knowledge or consent." (*Id.* at FIC001345.)

15. The Policy's "Forgery Coverage" covers "direct loss sustained by an **Organization** resulting from **Forgery** or alteration of a **Financial Instrument** committed by a **Third Party**" and provides a non-exclusive list of examples. (*Id.* at FIC001342.)

16. The Policy defines "**Forgery**" as "the signing of the name of another natural person . . . with the intent to deceive . . . . Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures." (*Id.* at FIC001345.)

17. The Policy is a standard form policy sold by Federal to many policyholders. (Ex. Stip. Ex. 22, Deposition of Christopher Arehart 40:20-41:4, July 9, 2015 ("Arehart Dep.").)

18. The terms and conditions of the Policy, including the endorsements, were entirely drafted or selected by Federal. (*Id.* 40:7-12, 43:10-44:2.)

19. The terms and conditions of the Policy, including the endorsements, were not the product of any negotiation between Medidata and Federal. (*Id.* 43:10-44:2.)

20. The Policy does not include the word "hacking" or any derivation thereof. (*Id.* 60:17-61:2; Ex. Stip. Ex. 23, Deposition of Michael Maillet 167:2-10, July 9, 2015 ("Maillet Dep.").)

II. <u>Medidata's Email System</u>

21. Medidata uses Google's Gmail platform for its corporate email system. (Affidavit of Glenn Watt, dated Aug. 11, 2015 ("Watt Aff.") ¶ 2.)

22. Medidata employees have email addresses with the domain name "mdsol.com," not "gmail.com." (*Id.* ¶ 3.)

23. Preceding "@mdsol.com," Medidata employees' email addresses generally consist of their first initial and last name. (*Id.*)

24. When a person emails a Medidata employee at their Medidata email address, the message goes to Google computer servers, where it is processed and then stored on those servers. (*Id.* ¶ 4.)

25. Google's servers that process and store Medidata's email constitute input, output, processing, storage, off-line media library and communication facilities that are utilized by Medidata, and are connected to computers that are owned and operated by Medidata. (*Id.* ¶ 5.)

26. After an incoming email is processed, Google's servers then enable it to be displayed in the Medidata employee's email account. (*Id.* ¶ 7.)

27. Medidata employees can access their email accounts on computers in Medidata's offices. (*Id.* ¶¶ 6-7.)

28. The computers in Medidata's offices are owned by Medidata. (*Id.* ¶ 7.)

29. When the information in an incoming email is processed by Google's servers, the Gmail system displays the sender's email address in the "From" line of the email. (*Id.* ¶ 8.)

30. One feature of Gmail is that Google's email system will compare an incoming email's sender's email address to all Medidata employee profiles contained in its system for a match. (*Id.* ¶ 9.)

31. If Google's Gmail system matches the email address of a sender with a Medidata employee account, it will display the sender's full name in the "From" line of the email, followed by the sender's "mdsol.com" email address. (*Id.* ¶¶ 8, 10.)

32. If Google's Gmail system matches the email address of a sender with a Medidata employee account to which a picture has been added, the email system will automatically display that picture next to the sender's name and email address in the "From" line. (*Id.* ¶ 10.)

33. Google's Gmail system will not, however, automatically add an electronic signature to emails based on the address of the sender. (*Id.* ¶ 11.)

34. Instead, each individual Medidata employee has the option to add an electronic signature to that employee's emails. (*Id.*)

35. Then, only emails initiated from that employee's actual Gmail account will automatically attach the selected electronic signature. (*Id.*)

III. **The Fraud Perpetrated against Medidata**

36. In the summer of 2014, company leadership briefed employees in Medidata's finance department on short-term plans for the future of the company, and emphasized possible acquisitions. (Ex. Stip. Ex. 19, Deposition of [redacted] 36:25-37:17, June 24, 2015 ("[redacted] Dep."); Ex. Stip. Ex. 21, Deposition of [redacted] 21:2-8, 34:22-35:12, June 25, 2015 ("[redacted] Dep."); Ex. Stip. Ex. 20, Deposition of [redacted] 22:24-24:2, 25:2-19, June 25, 2015 ("[redacted] Dep.").)

37. Personnel in the company's finance and accounting departments were told to be prepared to assist with significant transactions on an urgent basis. ([redacted] Dep. 36:25-37:17; [redacted] Dep. 21:2-8, 34:22-35:12; [redacted] Dep. 22:24-24:2, 25:2-19.)

38. At 11:12 AM on September 16, 2014, Medidata [redacted] employee [redacted] received an email (the "11:12 Email") from an imposter purporting to be Medidata [redacted] (the "Imposter"). (Ex. Stip. Ex. 2, at MED_0000816.)

39. [redacted] is [redacted] real email address at Medidata. (Watt Aff. ¶ 12; Maillet Dep. 78:4-15.)

40. [redacted] did not send the 11:12 Email. (Watt Aff. ¶ 12.)

41. The email address of the sender of the 11:12 Email was fraudulently manipulated to appear as if it was sent by [redacted] real email address at Medidata. (Ex. Stip. Ex. 2, at MED_0000816.)

42. The 11:12 Email was sent by a Third Party as defined by the Policy in a scheme to defraud Medidata. (Maillet Dep. 153:4-10.)

43. In a genuine email, the email address of the sender is accurately displayed in the "From" line of the email when viewed by the recipient. (Maillet Dep. 34:7-15.)

44. The "From" line of an email constitutes a representation of information, i.e., the email address of the sender of the email. (Maillet Dep. 57:11-17.)

45. The 11:12 Email was fraudulent, in part because the email address in the "From" line was not the actual email address of the sender of the email. (Watt Aff. ¶ 12.)

46. When Google's server processed the 11:12 Email that had been entered into its system, it recognized the sender's email address as [redacted], and consequently displayed the following in the email's "From" line: [redacted] (Watt Aff. ¶ 8; Ex. Stip. Ex. 2, at MED_0000816.)

47. Because Google's server recognized the sender's email address as [redacted], it consequently displayed [redacted] picture next to [redacted] name in the 11:12 Email. (Watt Aff. ¶¶ 9-10; Ex. Stip. Ex. 2, at MED_0000816.)

48. The 11:12 Email contained the electronic signature "[redacted]." (Ex. Stip. Ex. 3, at MED_0002113.)

49. The 11:12 Email was the first in a series of causal events that resulted in the transfer of $4,770,226.00 to an account designated by the perpetrators of the fraud and Medidata's subsequent loss of those funds. (Maillet Dep. 103:24-104:18.)

50. At 3:01 PM, [redacted] emailed the Imposter and Fake Attorney and explained that two authorized signatories would be required to send a wire from Medidata's JPMorgan Chase account. (Ex. Stip. Ex. 5, at MED_0002096.)

51. [redacted] identified a list of authorized signatories, including [redacted], and [redacted]. (*Id.*; [redacted] Dep. 11:3-5; [redacted] Dep. 9:22-24.)

52. [redacted] explained to the Fake Attorney that she needed any wire instruction to come from [redacted] himself. ([redacted] Dep. 34:14-21.)

53. At 3:32 PM, the Imposter sent an email to [redacted], and [redacted] (the "3:32 Email"). (Ex. Stip. Ex. 6, at MED_0001025.)

54. The email address of the sender of the 3:32 Email was fraudulently manipulated to appear as if it was sent by [redacted]. (Watt Aff. ¶ 12; Ex. Stip. Ex. 6, at MED_0001025.)

55. When Google's server processed the 3:32 Email that had been entered into its system, it recognized the sender's email address as [redacted], and displayed the following in the email's "From" line: [redacted] (Watt Aff. ¶ 8; Ex. Stip. Ex. 6, at MED_0001025.)

56. Because Google's server recognized the sender's email address as [redacted], it consequently displayed [redacted] picture next to [redacted] name in the 3:32 Email. (Watt Aff. ¶¶ 9-10; Ex. Stip. Ex. 6, at MED_0001025.)

57. The 3:32 Email instructed [redacted] and [redacted] to approve the wire [redacted] would prepare in the JPMorgan Chase wire transfer system. (Ex. Stip. Ex. 6, at MED_0001025.)

58. The 3:32 Email contained the electronic signature "[redacted]" (*Id.* Ex. 7, at MED_0002095.)

59. At 3:52 PM, the Imposter sent an email to [redacted] (the "3:52 Email"). (*Id.* Ex. 8, at MED_0001045.)

60. The email address of the sender of the 3:52 Email was fraudulently manipulated to appear as if it was sent by [redacted] real email address at Medidata. (Watt Aff. ¶ 12; Ex. Stip. Ex. 8, at MED_0001045.)

61. When Google's server processed the 3:52 Email that had been entered into its system, it recognized the sender's email address, and displayed the following in the email's "From" line: "[redacted]" (Watt Aff. ¶ 8; Ex. Stip. Ex. 8, at MED_0001045.)

62. Because Google's recognized the sender's email address, it consequently displayed [redacted] picture next to [redacted] name in the 3:52 Email. (Watt Aff. ¶¶ 9-10; Ex. Stip. Ex. 8, at MED_0001045.)

63. The 3:52 Email instructed [redacted] to wire $4,770,226.00 to Tongle Group HK Co Limited, Shanghai Pudong Development Bank Account No. OSA11443632717145. (Ex. Stip. Ex. 8, at MED_0001045.)

64. The 3:52 Email contained the electronic signature "[redacted]" (*Id.* Ex. 9, at MED_0002089.)

65. Taken together, the 11:12 Email, the 3:32 Email, and the 3:52 Email constitute instructions from the Imposter to transfer $4,770,226.00 to the account designated in the 3:52 Email. (Maillet Dep. 86:18-23.)

66. [redacted] used the beneficiary details from the 3:52 Email to prepare the wire in the JPMorgan Chase online system. ([redacted] Dep. 47:2-8.)

67. [redacted], and [redacted] confirmed to their satisfaction that the instruction came from [redacted] before they proceeded with their roles with respect to the transfer. ([redacted] Dep. 64:12-65:2; [redacted] Dep. 67:9-68:3; [redacted] Dep. 29:17-25.)

68. At 4:33 PM [redacted] approved the wire in the JPMorgan Chase online system. (Ex. Stip. Ex. 10, at MED_0000021.)

69. At 4:35 PM [redacted] released the wire. (*Id.*)

70. $4,770,226.00 was transferred from Medidata's JPMorgan Chase account to the account identified in the 3:52 Email. (*Id.* at MED_0000020.)

71. The $4,770,226.00 was transferred without Medidata's knowledge or consent. (Watt Aff. ¶ 12.)

72. Medidata did not purchase or receive anything in exchange for the funds transferred. (Maillet Dep. 179:19-180:2.)

73. The fraud was not caused by any fraudulent, dishonest, or criminal act by an authorized representative of Medidata. (Maillet Dep. 125:12-20.)

IV. **Medidata's Claim for Coverage**

74. Medidata made a claim under the Policy for the lost funds. (Ex. Stip. Ex. 11, at FIC000733.)

75. Federal employee Michael Maillet ("Maillet") investigated the claim. (Maillet Dep. 21:18-22:8.)

76. Maillet has the most experience of any Chubb claims examiner with respect to email fraud claims. (Maillet Dep. 105:25-106:6.)

77. Maillet confirmed that Medidata employees "acted upon a series of fraudulent emails purporting to be from the [redacted] of Medidata, [redacted] . . . ." (Ex. Stip. Ex. 12, at FIC000045; Maillet Dep. 42:15-43:11.)

78. Maillet requested a large amount of information, all of which, with the exception of certain privileged communications between Medidata and the outside counsel it hired to investigate the fraud, was turned over to Federal. (Ex. Stip. Ex. 13, at FIC000714; Maillet Dep. 136:20-137:2.)

79. On December 24, 2014, Federal denied coverage for the Claim, stating that coverage was not available under the Computer Fraud Coverage, the Funds Transfer Fraud Coverage, or the Forgery Coverage. (Ex. Stip. Ex. 12, at FIC000045.)

80. Federal denied coverage under the Computer Fraud Coverage because it believed there was no "fraudulent entry of **Data**" because the email inboxes of the Medidata employees were open to the public, and no "change to **Data** elements" because it found no evidence that the perpetrators of the fraud changed any preexisting data in committing the fraud. (*Id.* at FIC000048-49.)

81. Federal denied coverage under the Funds Transfer Fraud coverage because it found the wire transfer was authorized by Medidata employees and made with the knowledge and consent of Medidata. (*Id.* at FIC000049.)

82. Federal denied coverage under the Forgery Coverage because it argued that the emails were not signed, and even if they were, they did not meet the Policy definition of a Financial Instrument. (*Id.* at FIC000048.)

83. For both the Forgery Coverage and the Computer Fraud Coverage Federal also maintained the emails did not directly cause Medidata's loss, because had Medidata employees not acted upon the emails there would have been no loss. (*Id.* at FIC000048-49.)

84. Medidata is an "**Organization**" as defined in the Policy. (*Id.* Ex.1, at FIC001346, 1340.)

85. The perpetrators of the fraud are "**Third Parties**" as defined in the Policy. (*Id.* at FIC001347; Maillet Dep. 125:12-20.)

86. The $4,770,226.00 transferred from Medidata to the bank account designated by the perpetrators of the fraud and not subsequently recovered constitutes a loss of "**Money**" as defined in the Policy. (Ex. Stip. Ex. 1, at FIC001346.)

87. The Google servers and connected Medidata computers meet the Policy definition of "**Computer System**." (Ex. Stip. Ex. 1, at FIC001374.)

Dated: New York, New York
August 13, 2015

KASOWITZ, BENSON, TORRES &
FRIEDMAN LLP

By: ______________________________
Robin L. Cohen (rcohen@kasowitz.com)
Adam S. Ziffer (aziffer@kasowitz.com)
Alexander M. Sugzda
(asugzda@kasowitz.com)

1633 Broadway
New York, New York 10019
Tel: (212) 506-1700
Fax: (212) 506-1800

Attorneys for Plaintiff Medidata Solutions, Inc.